



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,111	03/25/2004	Jonathan Wilkins	MS#307312.01 (5104)	6640
38779 7590 01/22/2008 SENNIGER POWERS LLP (MSFT) ONE METROPOLITAN SQUARE, 16TH FLOOR ST. LOUIS, MO 63102			EXAMINER YOUNG, NICOLE M	
			ART UNIT 2139	PAPER NUMBER
			NOTIFICATION DATE 01/22/2008	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@senniger.com

mn

Office Action Summary	Application No. 10/809,111	Applicant(s) WILKINS ET AL.	
	Examiner Nicole M. Young	Art Unit 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5-24 and 26-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 and 26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This communication is in response to the amendment to application 10/809,111 filed on November 13, 2007. Claims 1-3, 5-24, and 26-40 are currently pending. Claims 4 and 25 have been cancelled. Claims 1, 8, 9, 15, 16, 21, 22, 26, 29, and 33-40 are amended. The Applicant has used the phrase "means for" within the claim language. The Examiner considers 112 6th paragraph to be invoked.

Claim Objections

The claims have been amended and objections of claims 14, 20, and 40 are withdrawn.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 16, 26, 33 are non-statutory because they do not produce a tangible result.

These claims end with comparing data, determining, or analyzing data. This does not provide a tangible result.

The claims have been amended and the rejection is withdrawn.

Claims 8-10, 21, 22, 25, 29, and 36-38 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The claims have been amended and the rejection is withdrawn.

Claims 25 and 32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 25 has been cancelled and the rejection is withdrawn. The rejection of claim 32 is withdrawn.

Claims 15 and 33-40 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The claims have been amended and the rejection is withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 5, 8-10, 13-17, 20-22, 26-27, 29, 30, 32-34, 36-38, 40 rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruton, III et al. (US 2003/0145225)**

herein referred to as Bruton, and further in view of **Hardman et al. (US 2004/0059941)**

herein referred to as Hardman.

Claims 1, 15, 16, 26, 30, 32, and 33 disclose a method of detecting an attack on an authentication service, said method comprising:

storing data relating to a plurality of requests (Figure 3, IDS Mgmt System 300 and associated text, also see Figure 4, 410) as communicated to an authentication service from a plurality of user agents via a data communication network (Figure 3 shoes multiple agents such as 230, 240 and 310 communicating with 300 over networks), said requests each including a password, and wherein storing the data relating to the requests comprises storing the password of each of the requests only if the request is unsuccessful;

searching the stored data based on a query variable to identify at least one of the plurality of the requests communicated from at least one of the plurality of the user agents (Paragraph [0057] wherein the packets are the stored data and the signature file is interpreted to be the query variable),

comparing the stored data associated with the identified request with a predefined pattern characterizing an attack based on the stored password of the identified request to determine when the identified request indicates the characterized attack on the authentication service (Paragraph [0057], the data is compared against the specific attack signatures which are interpreted to be predefined patterns characterizing an attack); and

detecting the attack in response to determining that the identified request indicates the characterized attack.

Bruton does not teach said requests each including a password, and wherein storing the data relating to the requests comprises storing the password of each of the requests only if the request is unsuccessful.

Hardman teaches said requests each including a password, and wherein storing the data relating to the requests comprises storing the password of each of the requests only if the request is unsuccessful (Hardman paragraph [0064] "the user name and password from a prior failed attempt to authenticate are stored on content server 110").

It would be obvious to one of ordinary skill in the art at the time the invention was made to store the user name and password from a prior failed attempt, since in Hardman paragraph [0064] states "a subsequent attempt to authenticate uses an identical user name and password, the process of flow diagram 200 is not repeated as it would provide the same result".

Claims 2, 17, 27, and 34 discloses the method of claim 1, wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following: a network address from which one of the plurality of the requests is communicated (Paragraph [0060] teaches address spoofing); a credential type of the one of the plurality of the requests; a user account associated with the one of the plurality of the requests (Paragraph [0074] where the IDS functions on the application layer) ; a status

of the one of the plurality of the requests (Paragraph [0029], wherein the conditions are interpreted to be the status of the event); a time stamp indicating a date and time of the one of the plurality of the requests (Paragraph [0035] teaches a date and time timestamp); a type of interface from which the one of the plurality of the requests is communicated; and the user agent from which the one of the plurality of the requests is communicated (Paragraph [0074] where the IP headers are interpreted to be the user agents).

Claim 3 discloses the method of claim 2, wherein said status of the one of the plurality of the requests comprises one of more of the following: the one of the plurality of the requests is successful; the one of the plurality of the requests is unsuccessful; and the user account associated with the one of the plurality of the requests has been locked (Paragraph [0068] teaches denying or discarding traffic that is determined to be related to an intrusion attack. This is interpreted to be a unsuccessful request).

Claim 5 discloses the method of claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using a single password to unsuccessfully attempt at least a predetermined quantity of requests on multiple user accounts within a predefined time interval; using the single password to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the multiple user accounts within the predefined time

interval; and unsuccessfully attempting at least the predetermined quantity of the requests from the single network address within the predefined time interval (Paragraph [0061] where the number of events from a single source are compared to a threshold).

Claims 8, 21, 29, 36 disclose the method of claim 1, further comprising generating a report if it is determined that one or more of the identified requests indicate the characterized attack, said report providing information regarding the attack for use in defending against the attack (Paragraph [0068] teaches reporting the intrusion events so that defensive action can be taken).

Claims 9, 22, and 37 disclose the method of claim 1, further comprising remedying the attack if it is determined that one or more of the identified requests indicate the characterized attack (Paragraphs [0068] and [0069] teach reporting the actions and ways to remedy the attack).

Claims 10 and 38 disclose the method of claim 9, wherein said remedying the attack comprises performing one or more of the following: locking a user account associated with one of the plurality of the requests; blocking a network address from which the one of the plurality of the requests is communicated; implementing a human interaction proof on the authentication service; prompting a user to change a password associated with the user account; and limiting a quantity of allowed unsuccessful requests to a predetermined quantity within a predefined time interval for the network address from

which the one of the plurality of the requests is communicated (Paragraph [0068] teaches methods of real time defensive actions in response to the attack).

Claim 13 discloses the method of claim 1, wherein said comparing the stored data associated with each of the identified requests with a predefined pattern comprises:

comparing historical data relating to the authentication service with the stored data, and

in response to said comparing, determining if the stored data deviates from the historical data to determine if the attack on the authentication service has occurred (Paragraph [0069] teaches writing attack events to a system log and comparing new events to the log to determine if the new events constitute normal or abnormal behavior).

Claims 14, 20, 40 discloses the method of claim 1, wherein said searching the stored data to identify at least one of the plurality of the requests comprises searching the stored data to generate a result set based on one or more of the following query variables: a network address that communicates an request, a quantity of user accounts for which access has been attempted, a password associated with a failed request, a quantity of failed requests for one or more user accounts, a quantity of requests for one or more user accounts (Paragraph [0110] teaches different sensitivity levels according to types of attacks), and a time interval during which one or more requests are communicated (Paragraph [0061] where the number of events from a single source are

compared to a threshold); wherein the result set identifies the stored data relating to one or more requests that correspond to the query variables (Paragraph [0083] and [0084] teach the signature files organized according to type of attack).

Claims 4, 6, 7, 18, 19, 28 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruton, III et al. (US 2003/0145225)** herein referred to as Bruton, as applied to claims **1-3, 5, 8-10, 13-17, 20-22, 25-27, 29, 30, 32-34, 36-38, and 40** above, and further in view of **Brock et al. (US 2003/0009693)** herein referred to as Brock and **Hardman et al. (US 2004/0059941)** herein referred to as Hardman.

Bruton and Hardman teach the limitations of claim 3 as rejected above. Bruton does not teach but Brock teaches **claim 4** which discloses the method of claim 3, wherein said storing the data relating to the plurality of the requests comprises storing a password associated with the one of the plurality of the requests if the one of the plurality of the requests is unsuccessful (Bruton paragraph [0004] wherein the pattern of bits is interpreted to be the password associated with the password log-on failure). It would be obvious to one of ordinary skill in the art at the time of invention to count the number of times a user tries unsuccessfully to log-on. The motivation to combine would be in Bruton paragraph [0004], which teaches that the number of log-on attempts is counted and compared against a threshold of events. If the attempts are above the threshold, it is determined to be an intrusion attempt and defensive actions are taken as stated.

Bruton and Hardman teach the limitations of claim 1 as rejected above. Bruton does not teach but Brock teaches **claims 6 and 19**, which discloses the method of claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple passwords to unsuccessfully attempt at least a predetermined quantity of requests on a single user account within a predefined time interval; using the multiple passwords to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the single user account within the predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests on the single user account within the predefined time interval (Bruton paragraph [0004] wherein the pattern of bits is interpreted to be the password associated with the password log-on failure. Paragraph [004] also compares the number of times the log-on is unsuccessfully attempted within a certain time period.) It would be obvious to one of ordinary skill in the art at the time of invention to count the number of times a user tries unsuccessfully to log-on. The motivation to combine would be in Bruton paragraph [0004], which teaches that the number of log-on attempts is counted and compared against a threshold of events. If the attempts are above the threshold, it is determined to be an intrusion attempt and defensive actions are taken as stated.

Bruton and Hardman teach the limitations of claim 1 as rejected above. Bruton does not teach but Brock teaches **claims 7, 18, 28 and 35**, which disclose the method of

claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: a single password to unsuccessfully attempt at least a predetermined quantity of requests from multiple network addresses on a single user account within a predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests from the multiple network addresses on the single user account (Brock paragraphs [0031] and [0032] which teaches multiple intrusion attacks at different levels of importance). It would be obvious to one of ordinary skill in the art at the time of invention to compare the multiple intrusion attempts against the level of importance stored in the security policy. The motivation is Brock paragraph [0006], which teaches the importance of taking into account the historical data of attacks.

Claims **11, 12, 23, 24, 31, and 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruton, III et al. (US 2003/0145225)** herein referred to as Bruton and **Hardman et al. (US 2004/0059941)** herein referred to as Hardman as applied to claims **1-3, 5, 8-10, 13-17, 20-22, 25-27, 29, 30, 32-34, 36-38, 40** above, and further in view of **Tumey et al. (US 2002/0097145)** herein referred to as Tumey.

Bruton and Hardman teaches the limitations of claim 1 as rejected above. Bruton does not teach but Tumey teaches **claims 11 and 23**, which disclose the method of claim 1, wherein the plurality of the requests comprises one or more of the following types of

requests: authentication, registration, and password-reset; wherein one of the plurality of the requests is communicated via a human interaction proof; and wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following: a network address from which the one of the plurality of the requests is communicated, a process where the human interaction proof is implemented, a time stamp indicating a date and time of the one of the plurality of the requests, and the user agent from which the one of the plurality of the requests is communicated (Tumey paragraph [0033] where the human facial image data is interpreted to be the human interaction proof used for authentication). It would be obvious to one of ordinary skill in the art at the time of invention to use the biometric security of Tumey in the intrusion detection system of Bruton. The motivation to combine is in Tumey paragraph [0005] which teaches that facial recognition is noninvasive security to the user and effective at all times.

Bruton and Hardman teaches the limitations of claim 1 as rejected above. Bruton does not teach but Tumey teaches **claims 12, 24, 31, and 39** which disclose the method of claim 11, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple test strings to unsuccessfully attempt at least a predetermined quantity of requests on a single human interaction proof string within a predefined time interval; and using a single test string to unsuccessfully attempt at least the predetermined quantity of the requests on multiple

human interaction proof strings within the predefined time interval (Tumey paragraphs [0070] and [0071] which teach the use of multiple images to create a threshold for authentication. If the image does not fall within the threshold, it is discarded). It would be obvious to one of ordinary skill in the art to use multiple images to create a threshold for authentication. The motivation would be in Tumey paragraph [0072] which teaches that images may have erroneous verification results to do poor presentation of the user to the system's camera. It is best to create a threshold so as to create the best image for the security of the user.

Response to Arguments

Applicant's arguments with respect to claims 1, 16, 26, and 33 have been considered but are moot in view of the new ground(s) of rejection. The Applicant argues that the independent claims do not include the added limitation of storing the data relating to the requests comprises storing the password of each of the requests only if the request is unsuccessful. The Examiner has added the Hardman reference in response to the added limitation. The Hardman reference teaches storing the data relating to the requests comprises storing the password of each of the requests only if the request is unsuccessful in paragraph [0064], "the user name and password from a prior failed attempt to authenticate are stored on content server 110".

It would be obvious to one of ordinary skill in the art at the time the invention was made to store the user name and password from a prior failed attempt, since in

Hardman paragraph [0064] states "a subsequent attempt to authenticate uses an identical user name and password, the process of flow diagram 200 is not repeated as it would provide the same result". This reference is also applied to all other claims that depend from the independent claims.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Application/Control Number:
10/809,111
Art Unit: 2139


Page 15

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
1/10/2008


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100